Response from SecurityScorecard
Comment on
RIN 3235-AM89 ("Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure")

I. Introduction

SecurityScorecard, the global leader in cybersecurity ratings, welcomes the opportunity to comment on the Securities and Exchange Commission's (SEC) proposed rule on cybersecurity risk management, strategy, governance, and incident disclosure for public companies.[1] In particular, the SEC's proposed rule focuses on ensuring the availability and comparability of public company disclosures across industries.[2] The SEC's work in this area is critical as cybersecurity risks to public companies grow and executives, shareholders, and customers seek greater clarity about appropriate approaches to cybersecurity risk management. As Congressman Jim Langevin (D-RI) said during a recent House Committee on Homeland Security hearing, "shareholders should be able to distinguish between companies that take [cyber] seriously."[3]

In this submission, we review why third-party security ratings and assessments are a cost-effective, comprehensive, and standardized way for organizations to assess and manage their cybersecurity risks—and an increasingly important component of cyber risk management programs. We also recommend that the SEC:

- Require public companies subject to SEC reporting requirements to report on incidents across their digital supply chain that materially impact their own cybersecurity, including with respect to third-party risk (responding to Question 10);

[1] RIN 3235-AM89. Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure.
[2] Ibid., 11.
[3] House Committee on Homeland Security, "Mobilizing Our Cyber Defenses: Securing Critical Infrastructure Against Russian Cyber Threats," April 5, 2022, https://homeland.house.gov/activities/hearings/mobilizing-our-cyber-defenses-securing-critical-infrastructure-against-russian-cyber-threats.

- Require registrants to disclose updates of independent, metrics-driven risk assessments in their quarterly and/or annual reports (responding to Question 15);

- Require registrants to disclose third-party risk assessment scores as part of their disclosed cybersecurity policies, procedures, and governance (in response to Question 17);

- Recommend that registrants quantify their cybersecurity risk exposure through independent risk assessments that produce security ratings (in response to Question 42);

- Recognize that continuous monitoring and independent, metrics-driven risk assessments are an increasingly cost-effective, comprehensive, and standardized way for organizations to assess and manage their cybersecurity risks, given half of all data breaches occur through third-party connections (responding to Questions 44 and 45);

- Recommend security ratings as a cost-efficient and effective mechanism for board oversight of cybersecurity; and

- Recognize in general that organizations should employ continuous monitoring, including of vendors and supply chain companies, as a cybersecurity best-practice.

II. Security Ratings and Communicating Cyber Risk

In its proposed rule, the SEC seeks to "enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and cybersecurity incident reporting by public companies" subject to 1934 Securities Exchange Act requirements.[4] The SEC's proposed rule focuses on mandating reporting about "material cybersecurity incidents" and requiring periodic disclosures about registrant's cybersecurity risk management policies and board expertise and oversight.[5] It also emphasizes the consistency of presentation

[4] Ibid., 1.
[5] Ibid.

across public companies in different industries, to ensure comparability of disclosures.[6] This last point is critical in providing the SEC with an understanding of the nation's risk, not just the risk to individual companies.

In order to comprehensively understand and communicate organizational cybersecurity risk, however, companies must first understand what the risks are and be able to quantify and prioritize mitigation efforts of those risks. As Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly testified to Congress in 2021, "I think it's hard to say you've reduced risk unless you know how to measure it." SecurityScorecard wholeheartedly agrees. You can't manage what you can't measure, and you can't defend what you can't see.

To date, nearly all companies define that risk too narrowly, focusing nearly-exclusively on the risks to their own digital infrastructure, even though half of all cyber incidents occur through third-party digital connections.[7] The cyber threat environment and organizations' IT environments are also constantly evolving.

To manage all this cybersecurity risk, organizations cannot use a playbook that relies on static analyses and entirely qualitative objectives. Instead, they must continuously assess cybersecurity risk across their entire supply chain and vendor ecosystem and produce quantitative metrics to measure that dynamic risk in a standardized, actionable way.

Security ratings solve for both of these capability gaps by providing a quantifiable assessment of internal risk and continuous visibility of third party risk. That is why SecurityScorecard believes that security ratings are a necessary component for every cybersecurity policy and should be a required element of this rule.

Third-party assessments provide unique, valuable insights and metrics on an organization's cybersecurity posture and the credibility of its claims about that posture. When conducted independently, assessments validate for the public,

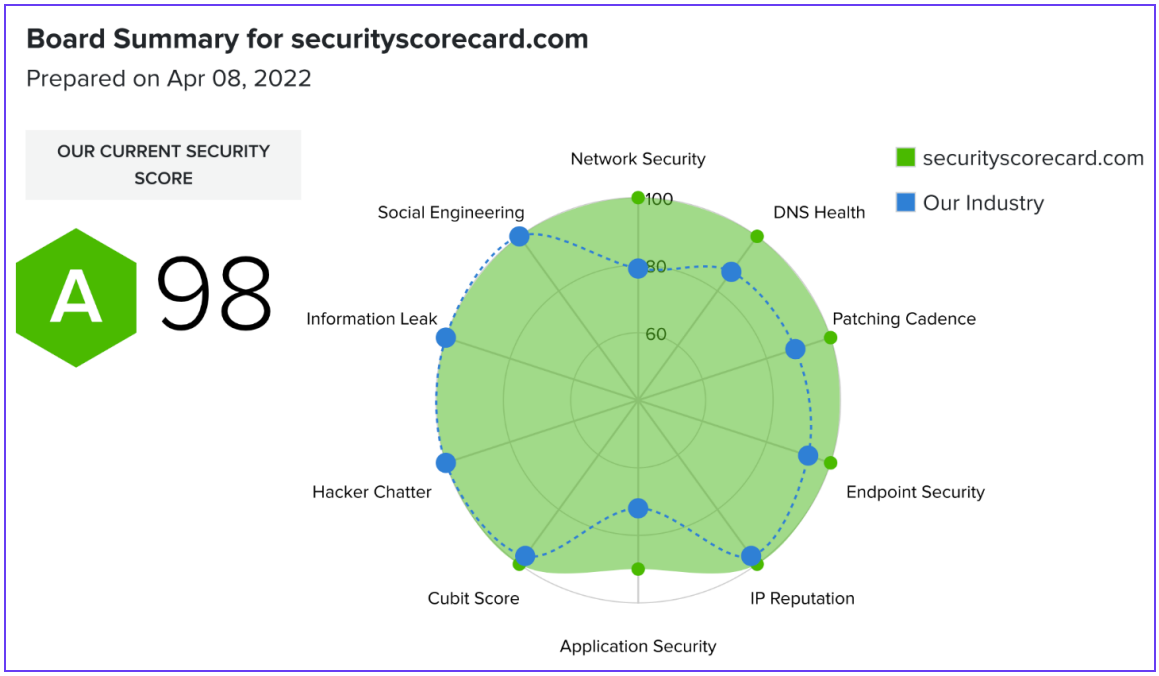
---

[6] Ibid., 11.

[7] "51% of organizations have experienced a data breach caused by a third-party," Security Magazine, May 7, 2021.

investors, third-party organizations like credit ratings agencies, and regulators that an organization is employing adequate cybersecurity measures. Especially when organizations are sourcing network and internet infrastructure components from a diverse and distributed global supply chain, third-party assessments can help an organization understand how these components affect its exposure to cybersecurity risks—to identify, analyze, and then mitigate those risks. As part of this process, security ratings provide organizations with quantifiable cybersecurity metrics that can be easily communicated and compared against other similar metrics.

Security ratings not only provide organizations with quantifiable cybersecurity metrics, ratings platforms like SecurityScorecard's, easily and automatically communicate cybersecurity risks to senior leaders and Board Members. In Fig. 1 (Board Summary for securityscorecard.com), we show an example of how our platform continuously monitors and maps cyber risk against the industry average across 10 Risk Group factors. The Board Summary provides an overall security score, and a cybersecurity health overview for your company and vendors. This automated reporting provides clear metrics for IT, C-suite, and Board of Directors leadership to track cyber risk and resource needs across the enterprise system, and make risk-based decisions based on the underlying data-driven analysis.



SecurityScorecard's A-F security ratings platform offers rigorous, free cybersecurity self-assessments to customers, and cost-effective assessments for their third-party vendors and suppliers. We conduct daily scans of the entire internet to map cybersecurity risk exposure and bring transparency to an organization's cyber hygiene. We do this without going behind any firewalls, only collecting public-facing data. We offer an "outside-in" perspective on an organization's security posture: we give organizations the ability to see what a hacker would see and are thus able to generate insights about the vulnerabilities, active exploits, and advanced cyber threats that a specific organization faces. Our customers use our platform not only to identify weaknesses in their own enterprise cyber hygiene, but to support their vendor risk management and supply chain security initiatives as well.

Figure 2

We generate our ratings (i.e., scores) by drawing on publicly available information, weighted and combined with historical data, to produce an objective security score. Importantly, this score, and the analytics behind it, change dynamically in response to changes in an organization's exposure to risks: if an organization's cyber hygiene starts to deteriorate, its score will suffer. While a high score does not translate to immunity from cyber risk, poor scores

are strongly correlated with increased likelihood of breach. This is unsurprising, as a poor score reflects that an organization has not sufficiently hardened its infrastructure against malicious actors, as the data in Fig. 2 reveals.

Our mission is "To make the world a safer place by transforming the way companies understand, improve, and communicate cybersecurity risks to their Boards, employees, and vendors." We offer a comprehensive picture of an organization's risk landscape alongside standardized, actionable security metrics. This kind of solution empowers organizations to accomplish many tasks:

- Continuously monitor their entire cyber risk exposure, including third-party vendors and suppliers;
- Choose the right Key Performance Indicators (KPIs) to prioritize and address cyber risk;
- Evaluate the effectiveness of existing internal security controls, tools, and processes;
- Identify potential gaps in security;
- Track remediation and mitigation efforts in real-over time;
- View cybersecurity progress improvements over time;
- Monitor and compare performance with industry competitors;
- Oversee third-party vendor cybersecurity; and
- Improve communication with vendors, regulators, and the board.

Security ratings are also cost-effective. Any organization can access their own security rating for free and scale their vendor risk management program to meet their needs. This is especially valuable for small- and medium-size businesses as well as local governments, who may not have the resources to employ a dedicated IT team or to contract IT services to defend their networks from cyber- and vendor-related risks. We can also help organizations to tailor their continuous monitoring and security metrics to their specific business needs. Security ratings are additionally cost-effective because they help build long-term capacity to manage cyber risk. As cyber threats evolve and as the IT environment changes, organizations can easily update security metrics in response—because they already have a risk assessment and security metrics framework in place.

Security ratings are especially powerful tools for board oversight of an organization's cybersecurity risk management. As an example of the crisp, easy-to-understand data that security ratings can furnish directors, we include a copy of the report that we provide to our board using our platform (Attachment 1).

For these reasons, security ratings are rapidly emerging as an essential element of cybersecurity risk management. According to CISA's then-Assistant Director for the National Risk Management Center:

> "The emergence of security ratings has driven cyber risk quantification as a way to calculate and measure cyber risk exposure. These security ratings provide a starting point for companies' cybersecurity capabilities and help elevate cyber risk to board decision making. Entities can also use security ratings alongside strategic risk metrics to align cyber scenarios with material business exposure; rollup cyber risks with financial exposure to inform risk management decisions; and measure improvement of cyber risk reduction over time. This kind of work needs to happen in the boardroom and also amongst national security leaders."

III. Recommendations

Security ratings should be an essential element of any organization's comprehensive strategy for managing cyber risks. Interconnected technology infrastructure sourced from a distributed, global, and diverse supply chain brings many possible risks. Static, point-in-time assessments of cybersecurity provided by a supplier are inadequate in a constantly evolving threat environment, and organizations in general may lack a comprehensive understanding of where a technology came from and its embedded risks. Security ratings also enable organizations to understand their own risk posture—screening an entire organization's digital and contractor supply chain to identify risks and quantitatively measure them.

Importantly, these measurements are cost-effective: technologies to perform them are widely available, and once organizations conduct one such assessment, subsequent assessments can build on those ratings to continually update cybersecurity risk assessments.

Third-party assessments, such as the security ratings offered by SecurityScorecard, can help public companies protect themselves and their customers against cybersecurity risks. Getting a more comprehensive, quantitative picture of an organization's digital supply chain empowers that organization to identify and target cybersecurity risks. Security ratings can also ensure that organizations better understand their network technologies while they procure them, before they deploy them, and as they maintain them. Further, security ratings provide a measurable, standardized, and cost-effective way of assessing an organization's cybersecurity, including vis-à-vis their contractor and digital supply chains.

10. [W]e are proposing to define cybersecurity incident to include an unauthorized occurrence on or through a registrant's "information systems," which is proposed to include "information resources owned or used by the registrant." Would registrants be reasonably able to obtain information to make a materiality determination about cybersecurity incidents affecting information resources that are used but not owned by them?

The answer is yes–registrants have cost-effective options for obtaining actionable insights into cybersecurity risks affecting their vendors and business partners. Accordingly, we recommend, in response to Question 10, that the SEC require registrants to report on incidents across their digital supply chain, including with respect to third-party risk. Security ratings platforms are an increasingly cost-effective way to survey an organization's entire digital supply chain and produce quantified, standardized security ratings. Hence, more organizations are using continuous monitoring and security ratings to monitor supply chain incidents. This kind of supply chain assessment—across vendors, contractors, third-party technologies, and other points of cyber risk to an organization—is critical to cybersecurity risk management.

Question 15. "Should we require registrants to disclose any material changes or updates to information … in the registrant's quarterly or annual report, as proposed?"

In response to Question 15, we recommend that the SEC require registrants to provide updates in the form of independent, metrics-driven risk assessments in

their quarterly or annual reports. Part of the value-add of security ratings is that they allow an organization to compare its current cybersecurity risk posture to previous points in time, as well as to that of competitors. By supplying updates to third-party risk assessments, registrants would provide boards and regulators with this kind of quantified cybersecurity risk rating to similarly assess the organization's current cybersecurity posture and its efforts to mitigate cybersecurity risk.

Question 17. "Are there other aspects of a registrant's cybersecurity policies and procedures or governance that should be required to be disclosed … to the extent that a registrant has [them]?"

In response to Question 17, we recommend that the SEC require registrants to disclose third-party risk assessment scores as part of their disclosures on cybersecurity policies, procedures, and governance. The SEC's proposal for Item 106 disclosures includes policies and procedures around cybersecurity (Item 106(b)), board and management oversight of cybersecurity (Item 106(c)), and cybersecurity incidents (Item 106(d)).[8] Independent, third-party risk assessments that produce security metrics empower organizations to monitor risk across their entire supply chain, as well as to understand and communicate that risk in a quantified fashion. These risk assessments across the supply chain are an increasingly essential part of cybersecurity risk management—and would provide useful information on a registrant's cybersecurity policies and procedures.

Question 42. "Would the proposed cybersecurity incident disclosure provide enough information for investors to assess the impact of a cybersecurity incident in making an investment decision? … Would investors benefit more if registrants were to provide the disclosure after the incident's impact is quantified or can be reasonably estimated?"

In response to Question 42, we recommend that registrants quantify their cybersecurity risk exposure through independent risk assessments that produce security ratings. Entirely qualitative cybersecurity risk assessments can be

[8] RIN 325-AM89. 92.

difficult to understand, challenging to verify, and hard if not impossible to compare directly to those from other organizations. Using quantified cybersecurity ratings, however, enables organizations to understand their risk numerically, map their risk over time and against competitors, and communicate that risk to stakeholders—from regulators to the board. Independent, third-party risk assessments are increasingly cost-effective, comprehensive, and standardized, helping organizations produce those kinds of quantified cyber risk metrics.

Questions 44-45. "Would the propose incident disclosure increase registrants' compliance costs to fulfill the proposed disclosure requirements related to incident reporting? … Would both types of the proposed disclosures lead to indirect economic effects for external stakeholders?"

In Questions 44 and 45, the SEC seeks comment on the possible compliance costs imposed on organizations by the proposed disclosure requirements. We recommend that the SEC recognize that continuous monitoring and independent, metrics-driven risk assessments are becoming lower-cost and more comprehensive—giving organizations an efficient and effective way to manage their cybersecurity risk. SecurityScorecard actually provides self-monitoring of a company's own digital footprint - the IP addresses that the company itself owns - for free to any organization. In addition, given that half of all data breaches occur through third-party connections,[9] security ratings that furnish insight into these risks are vital for maintaining a robust cybersecurity risk management program.

In considering proposed requirements for public companies to report on the board's cybersecurity expertise and oversight, we recommend that the SEC recommend security ratings as a cost-efficient and effective mechanism for demonstrating compliance. Given the general lack of cybersecurity expertise among corporate boards, quantified ratings of an organization's cybersecurity risk are easy for a board to understand and widely comparable to the ratings of competitors, others in the industry, and what are considered best-practices. SecurityScorecard couples its 1-100 security rating with an A-F grade that

[9] "51% of organizations have experienced a data breach caused by a third-party," *Security Magazine*, May 7, 2021, https://www.securitymagazine.com/articles/95143-of-organizations-have-experienced-a-data-breach-caused-by-a-third-party.

simplifies the information even further. Organizations can also generate security ratings on a continuous basis—including for boards to review—to demonstrate they are properly overseeing their risk posture and maintaining up-to-date cybersecurity risk management processes.

We also recommend that the SEC, in general, recognize that organizations should employ continuous monitoring as a cybersecurity best-practice. Static assessments of cyber risk in a complex world are insufficient to protect organizations and their users, vendors, and other constituents. This is especially so given that organizations have increasingly globally distributed and sourced technology supply chains—alongside complex relationships with third parties. Continuous monitoring, paired with independent and metrics-driven risk assessments, empowers organizations to understand their updated risk profile effectively and at low cost.

Respectfully submitted,
SecurityScorecard